Australian National University

CYBERSECURITY

MAPPING THE ETHICAL TERRAIN

National Security College Occasional Paper | No 6 June 2014

Nicholas G Evans, S Brandt Ford, Adam C Gastineau, Adam Henschke, Michael Keelty, Levi J West

National Security College

Crawford School of Public Policy

College of Asia & the Pacific

A joint initiative of the Commonwealth Government and The Australian National University

National Library of Australia Cataloguing-in-Publication entry

Authors: Evans, Nicholas G.
Ford, S. Brandt
Gastineau, Adam C.
Henschke, Adam
Keelty, Michael
West, Levi J.

Title: Cybersecurity: Mapping the ethical terrain [electronic resource] / Nicholas G. Evans, S. Brandt Ford, Adam C. Gastineau, Adam Henschke, Michael Keelty, Levi J. West.

ISSN: 2200-5269 (National Security College occasional papers)

ISBN: 978-1-925084-14-6 (ebook : pdf)

Series: National Security College occasional paper: 4 (Online).

Notes: Includes bibliographical references.

Subjects: National security--Australia.
National security--Australia--21st century.
Military planning--Australia.
Political leadership--Australia--21st century.
Australia--Politics and government--21st century.

Other Authors/Contributors:
Australian National University. National Security College.

Dewey Number: 355.0330994

Published and distributed by:
National Security College
Building 132a, 1 Lennox Crossing
Australian National University, Acton
ACT 0200
T: (02) 6125 6480
E: national.security.college@anu.edu.au
W: http://nsc.anu.edu.au/

CONTENTS

CONTRIBUTING AUTHORS

Nicholas G Evans

Dr Nicholas G Evans is a philosopher and bioethicist living in Philadelphia and an Adjunct Research Associate at the Centre for Applied Philosophy and Public Ethics, Charles Sturt University, Canberra. Dr Evans' primary research focus is the dual-use dilemma in the biological sciences, and ethical issues in regulating scientific research that poses a security threat to human health and wellbeing. His first volume on military ethics, the *Routledge Handbook of Ethics and War*, was published in 2013. He has also written on the ethics of emerging military technologies, professional ethics, public health ethics, and friendship. From January to March of 2014, Dr Evans was a visiting fellow at the Monash Centre for Human Bioethics in Melbourne; in July he will commence as a Postdoctoral Fellow in Advanced Biomedical Ethics at the Department of Medical Ethics and Health Policy, University of Pennsylvania.

Shannon B Ford

Shannon Brandt Ford is a Lecturer in Intelligence and Security Studies with the Australian Graduate School of Policing and Security, Charles Sturt University. Before starting his academic career, Mr Ford spent ten years as a Defence Strategist and Intelligence Analyst (1999-2009). He has taught at the Australian National University (ANU), the Australian Defence Force Academy (University of New South Wales) and the Australian Defence College. He has a Master of Arts (International Relations) from the ANU, and Bachelor of Arts (Psychology) and Master of Social Science (Criminology/Sociology) from the University of Queensland. He was a CAPPE Research Fellow on the ARC project 'Police Leadership in the 21st Century' and the Chief Investigator for the National Security College funded research project on the ethics of cybersecurity. Mr Ford's research interests include the theory and ethics of: cybersecurity; national security institutions (including military, police and intelligence agencies); leadership and strategy; intelligence studies; and analytical and critical reasoning in applied contexts.

Adam C Gastineau

Adam Gastineau is a PhD candidate focusing on police and military ethics with the Centre for Moral, Social, and Political Theory at the Australian National University. He has presented papers on the moral boundaries of police discretion and has also written on ethical issues pertaining to duty of care, targeted killing, the permissible use of lethal force *in bello*, and police corruption. He is currently working on a project examining the asymmetry between the norms governing the permissible use of lethal force by military personnel and those permitting the use of lethal force by police.

Adam Henschke

Dr Adam Henschke is a Research Fellow at the Australian National University's National Security College, an adjunct Research Fellow at the Centre of Applied Philosophy and Public Ethics, Charles Sturt University in Canberra, and was recently visiting Assistant Professor in the Department of Politics and Public Administration, University of Hong Kong. He started his academic career in the applied sciences, moved from biology to bioethics, completing a Master of Bioethics (2005–2006) at Monash University and a Master of Applied Ethics (2006–2007) at the Norwegian University of Technology and Linkoping University (Sweden). He was a researcher with the Centre for Human Bioethics at the World Health Organisation (2006), a visiting researcher at the 3TU Centre of Ethics and Technology at Delft Institute of Technology (2009), and a co-recipient of a Brocher Fellowship, researching ethical issues of 'Open Health' technologies in Geneva (2012). He has published in areas that include information theory, ethics of technology, and military ethics. He recently co-edited the *International Journal of Applied Philosophy*'s symposium on war in the 21st century (Fall 2012), *The Routledge Handbook of Ethics and War* (July 2013) and is currently co-editing a book on the ethics of cyberwarfare for the University of Oxford Press.

Michael Keelty

Mick Keelty, AO, APM, is an Associate Professor at the Australian Graduate School of Policing and Security, Charles Sturt University in Canberra and was Commissioner of the Australian Federal Police (AFP) from 2001 to 2009. He served two terms as AFP Commissioner and has thirty-five years of policing experience at local, national, and international levels. During this time, the AFP grew significantly, gaining major new responsibilities in counter-terrorism, high-tech crime, international peacekeeping and law enforcement capacity building. He also played a key role in the establishment of the Australian Crime Commission, which is a statutory body with Royal Commission-style powers established to tackle organised crime.

Levi J West

Levi West is Lecturer in Terrorism and National Security at the Australian Graduate School of Policing and Security, Charles Sturt University in Canberra. He coordinates the Masters program in Terrorism and Security Studies. Levi commenced his doctoral thesis at the Australian National University's School of International, Political and Strategic Studies in 2013. He is a graduate of the National Security College, holding a Graduate Certificate in National Security Policy, and Macquarie University's Centre for Policing, Intelligence, and Counter Terrorism, from which he holds Masters degrees in International Security Studies, and in Policing, Intelligence and Counter Terrorism. Levi's research is focused on the impact of technology on non-state actors, the evolution of terrorism and transnational crime, and cyber security. Levi has held various research and teaching positions in Australia and in the United States, the Middle East, and South Asia.

FOREWORD

Michael Keelty

Governments and society are increasingly reliant on cyber systems. Yet the more reliant we are upon cyber systems, the more vulnerable we are to serious harm should these systems be attacked or used in an attack. This problem of reliance and vulnerability is driving a concern with securing cyberspace. For example, a 'cybersecurity' team now forms part of the US Secret Service. Its job is to respond to cyber-attacks in specific environments such as elevators in a building that hosts politically vulnerable individuals, for example, state representatives. Cybersecurity aims to protect cyber-infrastructure from cyber-attacks; the concerning aspect of the threat from cyber-attack is the potential for serious harm that damage to cyber-infrastructure presents to resources and people.

These types of threats to cybersecurity might simply target information and communication systems: a distributed denial of service (DDoS) attack on a government website does not harm a website in any direct way, but prevents its normal use by stifling the ability of users to connect to the site. Alternatively, cyber-attacks might disrupt physical devices or resources, such as the Stuxnet virus, which caused the malfunction and destruction of Iranian nuclear centrifuges. Cyber-attacks might also enhance activities that are enabled through cyberspace, such as the use of online media by extremists to recruit members and promote radicalisation. Cyber-attacks are diverse: as a result, cybersecurity requires a comparable diversity of approaches.

Cyber-attacks can have powerful impacts on people's lives, and so—in liberal democratic societies at least—governments have a duty to ensure cybersecurity in order to protect the inhabitants within their own jurisdiction and, arguably, the people of other nations. But, as recent events following the revelations of Edward Snowden have demonstrated, there is a risk that the governmental pursuit of cybersecurity might overstep the mark and subvert fundamental privacy rights. Popular comment on these episodes advocates transparency of government processes, yet given that cybersecurity risks represent major challenges to national security, it is unlikely that simple transparency will suffice.

Managing the risks of cybersecurity involves trade-offs: between security and privacy; individual rights and the good of a society; and types of burdens placed on particular groups in order to protect others. These trade-offs are often *ethical* trade-offs, involving questions of how we act, what values we should aim to promote, and what means of anticipating and responding to the risks are reasonably—and publicly—justifiable. This Occasional Paper (prepared for the National Security College) provides a brief conceptual analysis of cybersecurity, demonstrates the relevance of ethics to cybersecurity and outlines various ways in which to approach ethical decision-making when responding to cyber-attacks.

First, Adam Henschke argues that we need to make decisions regarding cyber-attacks in a reasonable manner. Cybersecurity challenges involve a series of complex relations between old and new actors and old and new technologies. State security agencies have some duties to protect themselves and civilians against cyber-attacks. But to ensure that these duties are met in a way that is publicly justifiable, Dr Henschke argues that the decision procedures need to make explicit the moral values involved and how the state agencies make decisions between competing values.

Next, Nicholas Evans examines the argument, which proponents of the 'open culture' movement advocate, that with sufficient openness we enable others to solve modern challenges, including those posed to security in the information age. Here, Dr Evans presents a series of challenges to this argument; he offers only the most tentative of solutions, but hopes to move the discourse around openness and security on the internet from a series of technical hurdles to a set of ethical concerns.

Then Shannon Brandt Ford argues that we should be concerned about the use of cyberweapons because they have the potential to cause serious harm by attacking vulnerabilities in information systems. He demonstrates the way in which the distinction between 'war' and 'non-war' contexts is important for our understanding of the basic moral principles for justifying the use of cyberweapons. Importantly, he argues, proportionate and discriminate responses to cyber-attacks require the ability to distinguish an act of cyberwar from acts of cybercrime and/or cyber espionage.

Fourth, Adam Gastineau argues that cyber-surveillance greatly enhances a state's power to restrict the privacy of individuals. He argues, however, that the state is only permitted to restrict an individual's privacy through surveillance in cases where he or she can be shown to be liable to such restrictions. An individual's privacy is defined by the amount of access that others have to that individual. Restricting an individual's privacy without justification is wrongful, he argues, because it can unjustly restrict an individual's freedom. This restriction is only justified if one can be said to be a threat, and therefore liable to have their freedom restricted. Individuals who simply pose a risk are not sufficiently liable to have their freedom restricted in this way.

Finally, Levi West argues that cyberterrorism remains a contested and controversial concept, lacking definitional clarity. Cyberterror attacks on critical infrastructure offer poor return on investment for terrorist organisations, whose primary use of cyberspace remains focused on recruitment, radicalisation, financing and other network-sustaining functions. But it is possible, according to Mr West, to envisage future manifestations of cyberterrorism where data rather than people constitute the primary target, enabling, through the absence of conventional violence, more effective realisation of terrorists' political or ideological goals.

Australian National University

National Security College

A decision-making procedure for responding to cyber-attacks

Adam Henschke

National Security College

The National Security College is a joint initiative of the Commonwealth Government and The Australian National University

Introduction

Cybersecurity challenges involve a series of complex relations between old and new actors and old and new technologies. Furthermore, the decisions involved in responding or not responding to a cyber-attack will typically involve tensions between different morally important values. This presents decision makers with a challenge: how are we to respond to cyber-attacks in a way that is both practicable and ethically justifiable? This paper presents a general outline for an ethically based decision procedure for responding to cyber-attacks.[1]

Cyber-attacks can have powerful impacts on people's lives, and so in liberal democratic societies, governments are given a special duty to protect their citizens, and arguably, the people of other nations. In short, we generally expect governments to act to protect the security of people. But as recent examples involving the US National Security Authority (NSA) and the UK Global Communications Headquarters (GCHQ) have shown, there is public concern about what state security agencies do in pursuit of national security. Many potential cyber-attacks and responses pertain to ethical trade-offs: security vs. privacy, individual rights vs. an overall public good, the placing of burdens on particular groups over others. The critical reasoning tools found in practical ethics play an essential role in identifying where value conflicts arise, and offer ways of justifying responses that help to resolve such conflicts.

For example, a particular concern for securing cyberspace is the rise of dual-purpose infrastructure. Consider that something is targeted by a military attack. '[T]hat is, systems and structures for both civilian and military uses, or even civilian targets with the goal of demoralizing, weakening, or confusing an enemy's military and civilian leadership'.[2] The laws of war typically forbid the deliberate targeting of civilian infrastructure. But with a considerable amount of informational infrastructure being privately run for military use, or used by both military, industry and private actors, such discrimination between strictly military targets and strictly civilian targets becomes increasingly difficult.

Values and responses

The first aspect of a decision procedure is to develop a list of potential morally salient values that could potentially be in conflict. Box 1.1 (see below) contains a list of key moral factors that might be included in an anticipatory ethical decision-making procedure for responding to a cyber-attack.[3] Any list of such values is necessarily incomplete, and gives rise to a highly complex set of interactions between the different elements. As with the potential cyber-attacks themselves, the results of the interactions between the elements are hard to predict in advance, and it may be difficult to understand how they will play out through time.

1 This is intended to be a general outline only: any decision procedures for a specific cyber-attack would necessarily involve fine grained detail and would require extensive input, including – but not limited to – experts from computer science, security studies and applied ethics.

2 Randall R. Dipert, 'The Ethics of Cyberwarfare,' *Journal Of Military Ethics* 9, no. 4 (2010): 390.

3 Adapted from work by the following authors: Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst Publishers, 2013); Philip Brey, 'Anticipatory Ethics for Emerging Technologies,' *NanoEthics* 6, no. 1 (2013); Martin Libicki, 'Cyberdeterrence and Cyberwar,' (RAND Corporation, 2009).

Box One: Key Moral Values

- Just war principles
  - > response was proportional, discriminate, necessary, fair and not wrong in itself
- Risk to life
  - > Amount of people killed and/or severity of injuries
- Critical infrastructure
  - > Targets of attacks
  - > Non-life threatening (in the short term at least) but highly significant impacts
- Individual rights
  - > Cyber incidents and responses to them that violate individual's claims to:
    - > privacy
    - > property
    - > equality
- Trust
  - > Loss of trust in given service provider and/or system
  - > Loss of trust in security agencies/government/oversight, e.g., blowback from Edward Snowden actions
- Economic costs
  - > Direct economic theft
  - > Theft of intellectual property
  - > Redesign/rebuild critical infrastructure
- Efficiency
  - > May need to sacrifice efficiency for security, i.e. shift from 'just in time' service delivery to systems that offer a buffer, i.e. designing in system resilience, 'high availability'
  - > Raise consumer costs
  - > Basic annoyance i.e. constant password resets
- International relations
  - > Strain on diplomatic relations between nation states: Saudi Arabian/Israeli relations following 0x Omar data thefts, 2012.
- National security
  - > Trade individual rights for increased national security
  - > Require clarity on meaning of national security, i.e., is it maximised social good or private economic interest?
  - > Need to specify which rights are traded against national security, whose, and for how long.

The purpose of such a list is to present a set of morally salient values that may arise when formulating a decision procedure to respond to cyber-attacks. The first step in either designing an anticipatory decision procedure or determining how to respond to a given cyber-attack is to check the decision procedure against the list to see which values are in play, and which could potentially conflict.

General responses to cyber-attacks

The next step is to design a given set of responses. What a general ethical model can do is to postulate an 'if X, then Y' approach. Given the input of X, we anticipate the outcomes of Y, and then compare across different potential outcomes to assess which course of response is most ethically sound. By 'general', this methodology is intended to be neutral with regard to the particular ethical system being applied – it is agnostic with regard to favouring a particular style of consequentialism, deontology or other. The key aspect here is to make clear which set of values are guiding the decision making. The following is a description of reasoning from variable inputs, and then two visual models of the same set of reasoning.

if X cyber-risk will likely cause small economic harm,

then responding must not cause more economic harm (taking into account short-term and long-term economic costs)

AND

if Y responder (police investigation) has best capacity to respond to small economic harm,

then Y (police investigation) should be the responder

BUT

if X cyber-risk will likely cause significant harm to critical infrastructure

then identify responder with capacity: Military/Private

if military response has high moral hazard of acting/ medium moral hazard of not acting

AND

if the Private response has medium moral hazard of acting/medium moral hazard of not acting, then the Private response is most justified (all other things being equal).

Following Martin Libicki's position that one should differentiate between minimal impacts/economic impacts and high severity impacts on critical infrastructure,[4] I offer the following two models of response.

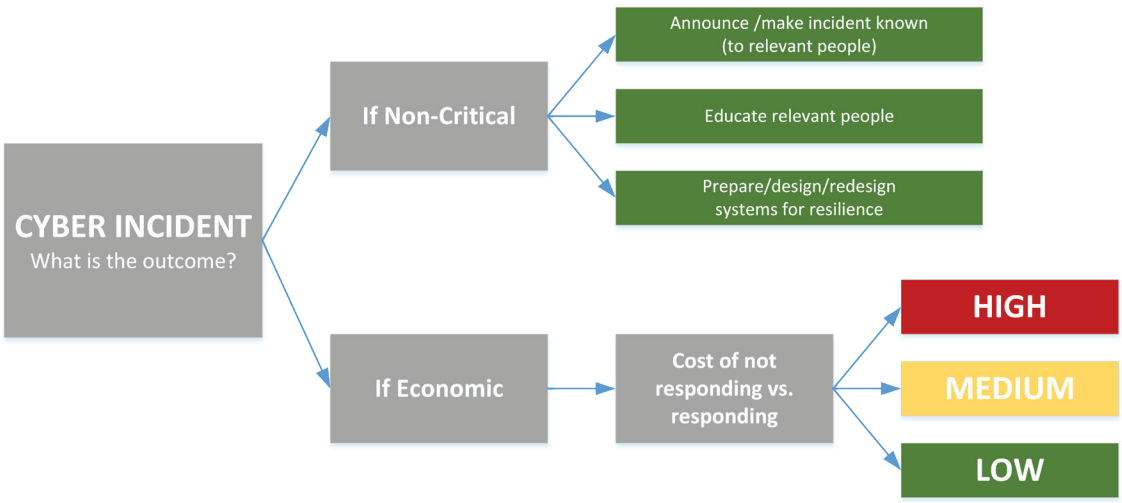

Figure 1: General response matrix to non-critical/economic harms

4 'Cyberdeterrence and Cyberwar.'

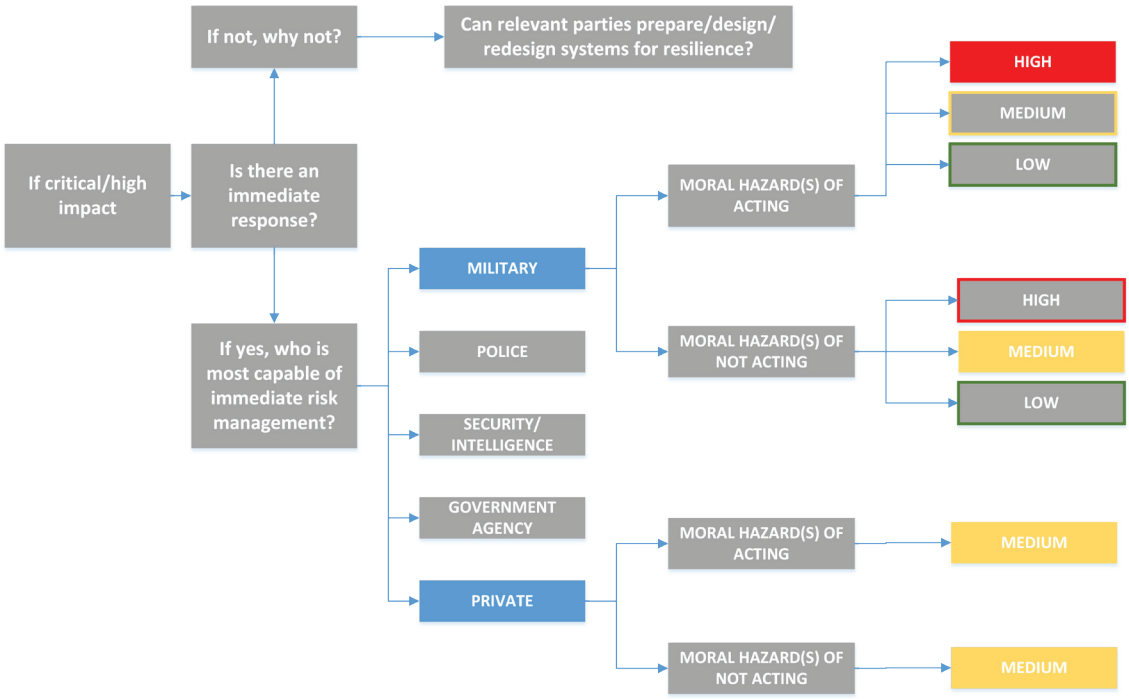

Figure 2: General response matrix to critical infrastructure/high impact attacks

Note that these are models only: they are deliberately simplified representations of methods of responding. They are not intended to replace the fine-grained and dynamic reasoning discussed throughout this paper. This point needs to be heavily emphasised, as there is a danger in simply applying this model, especially in conditions where there is uncertainty or limited time. Such models are suggested simplifications intended to provide a general indication of how ethical reasoning with relation to cybersecurity can operate in practice.

Second, to prescribed courses of action; the first matrix involves a cyber-attack on non-critical infrastructure, while the second involves a cyber-attack of high or severe impact or a circumstance that could impact critical infrastructure. As described earlier, one of the key elements of any effective cybersecurity program is the capacity to identify reliably the target and impact of a given cyber-attack. Despite fears of a cyber-Armageddon,[5] such an event has not occurred so far.[6] The point here is that we have typically encountered cyber-attacks that would be located in the first matrix. This is not to say that disasters cannot occur, but rather to point out that it is only the events in the second matrix that will typically require a major trade-off between key ethical values. Furthermore, if critical infrastructures can be designed such that cyber-attacks are likely to fall within the first matrix, then many of the challenging ethical decisions regarding cybersecurity can hopefully be avoided.

5 Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, (Harper Collins e-Books, 2010).

6 Rid, *Cyber War Will Not Take Place.*

In respect to the colour-coding, the models have been deliberately kept simple, with moral hazards given three potential ratings: green = low, orange = moderate and red = severe. If the set of potential outcomes includes all red and one green, then—absent significant extrinsic factors—the green option is the most favourable. Although any decision-making procedure must involve far more detail than that contained in these models, the point here is to illustrate what role ethical analysis can play in a given scenario. There is practical value to involving ethics in cyber-security, in a way that is central and foundational to decision making, rather than a patch or supplement at the end. As such, developing any decision procedures would need to involve consistent and high-quality ethical analysis such that the models do not replace effective decision procedures.

In this example, if X cyber-risk is likely to cause considerable harm to critical infrastructure, or have severe impacts on individuals, the second matrix is engaged. In the second matrix two courses of action have been identified—a military response and a private response. To spell out what this means, the comparison is between a military response, i.e., use of cyber-weapons and/or physical violence such as putting 'a missile down one of your smokestacks,'[7] and a private response, for example, a 'stand-your-ground' approach.[8] Again, this comparison is a deliberate simplification that highlights how comparisons can be made between different options. The two options, military and private, have been rated by reference to (a) immediate impacts, (b) moral hazards of acting/not acting, and (c) severity/impact—orange being moderate impact, red being severe. In situations of comparison, one can see that the impact of military action is severe, while that of private response is moderate. On this, it seems that private response is desirable to the military, but allowing private citizens to act might lead to escalation.

Such responses need integration. That is, what has been listed here is a simplified set of government agencies; military, police, security/intelligence, other government agency, and private actor(s). The 'if X, then Y' decision framework and resulting matrices imply coordination between government agencies and simplify these agencies to clusters such as 'military'. The reality of government is far more complex. The military, for example, is a highly complex institution comprising many different groups, sub-groups and actors. Consequently, what is necessary for effective cybersecurity is a coordinated level of integration and harmonisation between these agencies, perhaps overseen by a specific department such as the Australian Cyber Security Centre (ACSC). It might be that the chief organising department shifts over time, as it has done in the past,[9] but my point is that coordinated, integrated and harmonised responses are necessary for effective cybersecurity.

Developing long-term strategies for cybersecurity

In order to ensure a robust capacity to respond to cyber-attacks, I suggest that an integrated cyber-operations centre have the capacity to:

- identify relevant agencies with capacity and mandate to respond
- identify and recognise a given threat
- work within a clear chain of command
- identify moral hazards of acting/not acting in the short and long term.

7 This is a reference to a Pentagon official who made the now-famous statement in a *Wall Street Journal* article, 'If you shut down our power grid, maybe we will put a missile down one of your smokestacks', Siobhan Gorman and Julian E. Barnes, 'Cyber Combat: Act of War,' *The Wall Street Journal*, 31 May 2011.

8 Patrick Lin, "Stand Your Cyberground' Law: A Novel Proposal for Digital Security,' *The Atlantic*, 30 April 2013.

9 Peter Jennings and Tobias Feakin, 'Special Report – the Emerging Agenda for Cybersecurity,' (Canberra: Australian Strategic Policy Institute, 2013).

As part of a long-term strategy for cybersecurity, personnel also need effective education. This relates both to personnel working within the responsible agencies (including the people likely to become personnel) and the general public. Such education is essential. Social engineering involves cyber-attackers targeting humans as key points of vulnerability in a cybersecurity system. Some claim that up to 70 per cent of successful cybersecurity attacks involve social engineering.[10] One example involves leaving infected USB sticks on the ground outside a given agency or institution with the intention that staff pick up the infected USB stick and plug it into the institution's computers, thus potentially infecting the computer network and bypassing the air-gap. Education of staff and the public at large can go some way to reducing these sorts of vulnerabilities.

Some countries, such as The Netherlands, have proposed laws such that institutions have a duty to report cyber-attack incidents.[11] The motivation behind the duty to report is that all will benefit from the disclosure and sharing of cyber-incidents. A duty to report is a prime example of designing robustness into a system. But a key concern about a duty to report is that if a company is required to declare publicly its vulnerabilities and failures in its cybersecurity, then consumers and shareholders will flee the company, potentially causing the company to go bankrupt, as the incidents affecting the company DigiNotar demonstrate.[12] This is not an imagined scenario—public knowledge of cybersecurity failures has had highly negative impacts on given companies. Furthermore, the loss of public trust in a company with the aim of driving it out of business could in fact be the intended aim of the given cyber-incident. Any duty to report mechanisms must be carefully and thoughtfully designed.

With this in mind, the particular attributes of a duty to report would have to include who is reporting to whom, when, what the content of the report would require, which relevant industry actors should be alerted to the given incident, and just how such reports should be made public. A possible model here is in civil aviation, where the aviation industry has mandatory reporting requirements[13] but has systems in place that allow for in-confidence reporting. This means that all actors in the aviation industry benefit, those who have suffered incidents do not unjustifiably suffer, and the public retains trust in the system as a whole.

Conclusion: actions and reasons for acting

As the fallout from the leaks by Edward Snowden has shown, people around the world are now taking an interest in what states are doing in pursuit of national security. An important lesson to be learned from the Snowden revelations is that a reference to 'national security' alone is not sufficient to justify the actions of national security agencies. Making the values underpinning decision procedures more apparent is one way of ensuring that cybersecurity is not only achievable but also deemed acceptable to a state's citizens. The ethical decision-making process offered here can, hopefully, help formulate such a set of procedures.

10 Mark Bowden, *Worm: The First Digital World War* (New York: Atlantic Monthly Press, 2011).

11 Government of The Netherlands, 'New Legislation on the Duty to Report and Possibilities for Intervening in the Event of Digital Security Incidents,' Government Of The Netherlands, http://www.government.nl/news/2012/07/06/new-legislation-on-the-duty-to-report-and-possibilities-for-intervening-in-the-event-of-digital-security-incidents.html.

12 Rid, *Cyber War Will Not Take Place*, 26–30.

13 Civil Aviation Safety Authority, 'Safety Information Policy Statement,' Australian Government, http://www.casa.gov.au/scripts/nc.dll?WCMS:STANDARD:1001:pc=PC_101466.

Australian National University

National Security College

Cybersecurity and open, distributed cultures:
Designing in ethics

Nicholas G Evans

National Security College

The National Security College is a joint initiative of the Commonwealth Government and The Australian National University

Introduction

Two features[1] of modern cyberspace present a serious challenge for cybersecurity:

Distribution: information and communications technologies (ICTs) are most productive when ubiquitous[2]

Deskilling: the development of cyberspace has seen a proliferation of skill and access, enabling a larger number of people to command relatively large amounts of power in cyberspace.[3]

Distribution and deskilling create a security challenge by lowering the costs—material, experiential, and opportunity—of the malevolent use of technology. Committing acts ranging from minor vandalism to large-scale economic or physical harm is becoming ever more possible.[4] We are approaching a crisis point at which the cost of committing cybercrime[5]—in terms of technical and economic barriers—is very low; however, the consequences of individual acts can be quite large.

Dual-use and open access

This problem is neither new nor unique to ICTs, but finds expression in a number of contemporary problems of 'dual-use,' whereby one and the same technology or set of technologies can be used for good or evil.[6] As the cost of genomic sequencing – and increasingly, synthesis – falls, we encounter the widespread proliferation of accessible, powerful biotechnology.[7] Likewise, the ability to produce, modify, and even wrest control of drones is already in the public domain.[8] Convergent technologies such as 3D printing could further this convergence of ease of access, use, and modification.[9]

Each field has its risks, and ICTs present these risks in the most obvious fashion by virtue of the field's maturity. In point of fact, biotechnology is still very much considered science, while drones both find considerable research promise as well as an emerging market presence. ICTs are certainly the subject of research, but are also a mature, ubiquitous, and relatively well-functioning collection of technologies.

1 These features are not exhaustive of issues in cybersecurity; they are, however, significant challenges.

2 Weber, Steven, *The Success of Open Source*. Harvard University Press, 2005; Hope, Janet, *Biobazaar: the open source revolution and biotechnology*, Cambridge, MA: Harvard University Press, 2008; Carlson, Robert, 'The pace and proliferation of biological technologies,' *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, 1 (3), 2003, 203–214. Though this productivity is not always a good thing, see e.g., Goodman, M. 'A vision of crimes in the future,' *Technology, Entertainment, and Design (TED) Global*, June 2012 http://www.ted.com/talks/marc_goodman_a_vision_of_crimes_in_the_future.html (Accessed 6 July 2013). The subject of when innovation or productivity is truly good is for another paper currently under development, but it seems clear (and indeed that paper is motivated from the intuition) that not everything productive or innovative is indeed *good*.

3 De Joode, Ruben van Wendel, *Understanding Open Source Communities: An Organizational Perspective*. Doctor of Philosophy, TU Delft, Delft, NE, 2005.

4 Arquilla, John, 'Twenty Years of Cyberwar,' *Journal of Military Ethics* 12:1, 2013, 80–87.

5 Or cyberterrorism, though perhaps not (yet) cyberwar. I won't offer a comprehensive analysis of these terms and distinctions between them; the token I use for malevolent acts in cyberspace is cybercrime.

6 Evans, Nicholas G., 'Great expectations – ethics, avian flu and the value of progress,' *Journal of Medical Ethics* 39: 4, 2013, 209–13.

7 Hope, *Biobazaar*.

8 Carlson, Robert, 'Are These The Drones We're Looking For? (Part IV)' 11 October 2012 http://www.synthesis.cc/2012/10/are-these-the-drones-were-looking-for-part-iv.html (Accessed 28 November 2013)

9 The 'Drone It Yourself' project is an open-source, 3D printable drone platform that can use any regular object as a drone body. See http://jaspervanloenen.com/diy/ (Accessed 28 November 2013).

Assessing the risks

A comprehensive account of the current risks is beyond the scope of this paper, but a brief survey of recent events will demonstrate the type and pervasiveness of existing threats. Stuxnet, the worm that infected Siemens systems worldwide, but "mysteriously" only attacked and damaged Iranian nuclear centrifuges in 2010, is of course the paradigm of cyberwar.[10] In July of 2013, an English court ruled that Flavio Garcia, a researcher at the University of Birmingham, be banned from publishing his research on cracking the security systems of luxury cars; Volkswagen applied for an injunction against Garcia based on the security implications of his work.[11] While talking about cars, it should be noted that in 2010, collaboration between University of California San Diego and University of Washington showed that car software could be hacked, and malicious code embedded through most any system in a car, including the CD player.[12] Similarly, the Food and Drug Administration has warned that medical devices can be hacked.[13] GPS satellites are also at risk: Tyler Nighswander's team from Carnegie Mellon University showed that 20–30 per cent of the global Continuously Operating Reference stations could be rendered inoperable via malicious GPS broadcasts using about $2,500 worth of equipment.[14]

Everything and everyone is vulnerable, and the technical solutions to guard against such vulnerability can often be complex.[15] The more secure the system, the higher the barrier to penetration—but few systems are overly secure. Researchers recently discovered a critical vulnerability in the Android phone operating system that allowed attackers to inject malicious code into legitimate programs—and they identified instances 'in the wild' of attackers doing just that.[16]

These represent some emerging security issues in civilian devices; however, the majority of cybercrime—which costs hundreds of billions of dollars per year[17]—is performed through endemic but uncontroversial exploitation of computer systems around the world. In terms of individual losses, compromised critical infrastructure may be catastrophic. However, the current state of cybercrime is one that represents a massive loss distributed over a panoply of relatively minor losses. Importantly, a great deal of this crime is centralised through organised crime gangs, who have moved into the online world for its lack of accountability and enforcement.[18]

10 Lucas, George, 'Jus in Silico: Moral Restrictions on the Use of Cyberwarfare,' in Allhoff, Evans, and Henschke, *The Routledge Handbook of Ethics and War,* Routledge, 2013.

11 O'Carroll, Lisa, 'Scientist banned from revealing codes used to start luxury cars,' *The Guardian,* 27 July 2013, http://www.theguardian.com/technology/2013/jul/26/scientist-banned-revealing-codes-cars (Accessed 27 November 2013).

12 Koscher, Karl et al., Experimental Security Analysis of a Modern Automobile *IEEE Symposium on Security and Privacy*, May 2010.

13 US Food and Drug Administration, 'FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks,' 13 June 2013 http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm (Accessed 27 November 2013).

14 Nighswander, Tyler, Ledvina, Brent, Diamond, Jonathan, Brumley, Robert, Brumley, David, 'GPS Software attacks,' CCS '12 October 16-18, 2012, Raleigh, NC http://users.ece.cmu.edu/~dbrumley/courses/18487-f12/readings/Nov28_GPS.pdf (Accessed 28 November 2013).

15 Goodin, Dan, 'No easy way to stop BREACH from plucking secrets from HTTPS pages, feds say' 3 August 2013, http://arstechnica.com/security/2013/08/no-easy-way-to-stop-breach-from-plucking-secrets-from-https-pages-feds-say/ (Accessed 28 November, 2013).

16 Goodin, Dan, 'First malicious apps to exploit critical Android bug found in the wild,' 24 July 2013, http://arstechnica.com/security/2013/07/first-malicious-apps-to-exploit-critical-android-bug-found-in-the-wild/ (Accessed 28 November 2013).

17 For a good summary of the range of difficulties in estimating the costs of cybercrime, and some preliminary estimates, see Anderson et al., 'Measuring the Costs of Cybercrime,' 11th *Workshop on the Economics of Information Security*, (Berlin, July 26 2012).

18 McCusker, Rob, 'Transnational organised cyber crime: distinguishing threat from reality,' *Crime, Law and Social Change*, 46:4-5, 2006, pp.257-273. See also Williams, Philip 'Organized Crime and Cybercrime: Synergies, Trends, and Responses,' *Global Issues* 6:2, 2001, 22-26.

If crime is the threat, the true challenge arises in what one does about such widespread, accessible, distributed skill in a vulnerable environment. By virtue of their structure, distributed and deskilled endeavours are resistant to 'preventative' strategies—regulation, export controls, licensing and prohibition.[19] Distributed, deskilled communities have the ability to circumvent security strategies with ease—something we see in everything from the theft of 100 million SONY Playstation accounts, to Lulzsec, to the Arab Spring.

Prevention strategies are problematic, it is claimed, because they drive away talent; restrict access to materials, opportunities, and skills; and limit the freedom to innovate. They also routinely fail to protect individuals from harm: hampering beneficial innovation while failing to prevent misuse is the hallmark of failed regulation.[20]

Instead, proponents of distributed and deskilled cultures call for 'preparation' strategies: incentivising rapid, beneficial innovation combined—in some cases—with comprehensive technology monitoring. In very simplistic terms, preparation strategies create conditions in which the progress of those securing our good outpaces those who mean us harm.

The problem of regulation

Preparation is claimed to surpass prevention. Prevention is too sluggish for the environment on which it acts: it doesn't always fail, but it fails too frequently, or is too costly, to be a satisfactory solution. It is claimed that preparation is the superior strategy because it incentivises beneficial development—a desired end regardless of approaches—without spending on costly and ineffective regulation.

Yet preparation rests on the assumption that the "good guys" can be meaningfully faster than the "bad guys," and thus be a strategy that succeeds against other contenders. This is a highly problematic claim and I offer a series of concerns with holding such an assumption.

First: *numbers*. How do we ensure that there are enough good guys relative to bad guys to achieve sufficient security? The good guys need to cover all or most of their bases—bad guys only need to hit one target. This is a manpower issue: does an open system like the one described in the prevention strategy have the right incentives to attract people to solving security issues?

The answer, I think, is *no*. A typical response to the problem of malfunction or malfeasance in open systems is that that 'many eyes make all bugs shallow.' Distribution and deskilling increase the number of good guys, by virtue of leaving problems open for the largest possible number of people to work on.

This problem is larger still because bugs are *not* vulnerabilities.[21] Bugs are typically parts of a system that, when used, cause disruption in normal functioning. Vulnerabilities, however, do not present as disruptions in normal functioning up until the point that they are exploited. We need, then, enough good guys who are knowledgeable and relevantly incentivised to find vulnerabilities, and enough individuals that can shore those vulnerabilities up once they are found.

19 Carlson, Robert, *Biology is Technology: The Promise, Peril, and New Business of Engineering Life*, Cambridge, MA: Harvard University Press, 2010.

20 Carlson, *Biology is Technology*.

21 Laurie, B. (2005). 'Open Source and Security'. In C. DiBona, D. Cooper & M. Stone (Eds.), *Open Sources 2.0: The Continuing Evolution* (pp. 57–71). Sebastopol, CA: O'Rielly.

Second, relying on preparation makes certain assumptions about the uptake of information in an open system—namely, that it is comprehensive enough to penetrate society and secure the number of people (as above) with the *amount of skill* we need. But this is not assured as a matter of what it means for a system to be open in the way that distributed and deskilled communities are open. The whole *point* is to provide information, but that is not the same as education. Huge numbers of individuals use open-source software—56 per cent of the web server market is held by the open-source organisation the Apache Software Foundation.[22]

Yet the population of individuals with the skill to fix bugs, much less to repair security vulnerabilities, is surely very small in comparison.[23] Developers may be recalcitrant or reluctant to adopt security measures. Software may not be designed with security in mind. And the security risks keep on evolving—faster than people can keep up.[24]

Third and finally is the problem of what I will call 'parasitic malevolence.' Innovation in open communities, it seems, runs into the problem that even though secrecy is an unstable strategy,[25] it can limit information uptake to accelerate a security program sufficiently. In distributed, deskilled communities, we assume that for each innovation we make, that malevolent individuals cannot easily piggyback off our efforts. The degree to which this holds is in part the degree to which preparation strategies can succeed.

If part of our preparation strategy is to innovate along the lines of securing cyberspace, then perhaps this will work. But if the preponderance of innovation is directed towards new, unsecured endeavours in cyberspace—particularly when connected back to other important services, as in the case of Mat Honan of *Wired* magazine, whose Amazon account was hacked, and then daisy-chained into his Apple ID, Gmail and Twitter accounts. The hackers eventually locked Honan out of his computer and then wiped it clean—it is worth noting that the hackers used a customer service line to gain access to his iCloud account.[26]

Conclusion: how to proceed

Can the assumptions on which the preparation strategy is based be borne out, and if so, to what degree? If the answer is 'yes,' so much the better—particularly if preparation is low cost. But if not, or if successful preparation comes at a very high cost, this is a serious concern. It of course does not mean that the preparation strategy is a write off: it may still be our best option. But it should give us pause.

This is not merely a technical problem: it is a combination of technical and ethical conflicts. Preparation can lead to rapid innovation, but the rate of uptake of that innovation can vary greatly.[27] Early adopters and the highly educated benefit immensely, while the benefits to others decrease in proportion with their ability to use the technology, and to be integrated into the dynamics of the resultant culture.

22 Hope, *Biobazaar.*
23 Laurie, 'Open Source and Security.'
24 Bright, Peter, 'Crypto experts issue a call to arms to avert the cryptopocalypse,' 2 August 2013, http://arstechnica.com/security/2013/08/crytpo-experts-issue-a-call-to-arms-to-avert-the-cryptopocalypse/ (Accessed 28 November 2013).
25 Schneier, Bruce. Securing Medical Research: A Cybersecurity Point of View. *Science*, 336:6088, 2012, 1527-1529.
26 Honan, Mat, 'How Apple and Amazon Security Flaws Led to My Epic Hacking,' *Wired* 8 June 2013 http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/ (Accessed 28 November 2013).
27 Evans, 'Great Expectations'

If we rely on prevention only, we appear to be doomed to watch as open culture on the Internet 'routes around' damage. We drive away otherwise benevolent innovation while doing nothing to protect individuals from harm. We may even exacerbate the damage by causing more unrest—the harm caused by revelations of PRISM is yet to be seen, but already constitute a public relations disaster.

If we follow through with preparation, the concerns I raise need to be addressed. Rapid innovation requires empowering a great number of individuals to identify weaknesses: this is a coordination issue that has its own trade-offs. Letting the status quo remain is likely to result in a dearth of experts, but there are risks involved in creating security experts in terms of oversight and corruption. A society of skilled experts in ICT vulnerabilities must be accountable for their role in larger society, and when engaged in the highest levels of security, problems emerge. One form this corruption could take is the misuse of such an organisation by the state; the other form is that of individual corruption of members of that organisation, tempted to use their skills for more profitable ends.

Educating a populace is no doubt a good thing, but is a politically volatile subject in a number of jurisdictions. Moreover, allowing security needs to influence education would be, I suspect, unpalatable to many. It is also potentially time-consuming, costly, and high-risk. Ultimately, if individuals can limit their own vulnerability and be inured to the social aspects of cybercrime (eg, phishing) then there is less to worry about. But how much this would cost, and how to do this while preserving education in a range of other areas is a hugely complex question.

We will also need to educate law enforcement on a more distributed level, so that state and federal and international agencies can better react against cybercrime. As cybercrime becomes more distributed, and affects a greater number of devices (e.g., medical devices, vehicles etc.), we require greater know-how across the board. In societies in which policing is underfunded or neglected by the political process, or in which policing forces do not have the trust of their communities, this is incredibly problematic.

These are all, however, fixes that leverage the background institutions on which our society, and our use of technology, rest. The degree to which we are willing to allow preparation to proceed should be a function of our trust in these institutions, and of the degree to which we are willing to trade off the benefits preparation brings against other valuable goods. If our institutions fail us and we reach too far, the costs could be very high indeed.

Finally, parasitic malevolence provides a serious challenge to preparation. The seemingly obvious solution is community engagement, but this has had mixed results for reasons I've mentioned regarding trust in law enforcement. Surveillance can be problematic without community participation or consent, even if only in terms of backlash when surveillance is revealed.[28] However, the cultures about which we are talking are often divided about how to relate to problems of security and the function of the state in promoting security. This is a larger ethical issue that I cannot develop here, but which must also be tackled.

At the end of the day, preparation may be better that prevention. But in order to show that is the case with any degree of confidence, we need to know what we are promoting, what that trades off against, and whether that comprises an acceptable set of risks to take among an increasingly broad sector of society (i.e., internet users). When we begin comparing and trading off values we enter the domain of ethics; this suggests to me that mere technological innovation cannot be preparation enough—preparation must be designed with ethics in mind.

28 http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

Australian National University

National Security College

Warfare, cyberweapons and morality

Shannon B Ford

National Security College

The National Security College is a joint initiative of the Commonwealth Government and The Australian National University

Introduction

Cybersecurity is an increasingly prominent feature of the national security agenda. National governments are alarmed at the potential for serious attacks on cybersecurity and are responding accordingly. The Australian Government, for instance, nominated 'malicious cyber activity' as one of seven key national security risks in the 2013 Australian national security strategy.[1] Given such an emphasis on cybersecurity, and the significant investment governments are making in this area, clearly it is an important task to establish a firm conceptual grasp on what we mean by the term. After all, it appears that cybersecurity is being used in a very broad sense to capture everything that is happening in the cyber domain. In this sense, cybersecurity is 'an ill-defined catch-all for the nuanced problems of a tech-rich, hyper-networked world.'[2] Certainly, cybersecurity encompasses a range of conceptual axes: private and public infrastructure; threats against information or harms to or through physical devices. But cybersecurity can also be used in a more specific sense as protecting national cyber-infrastructure from threats to its reliability. For the purposes of this paper, cybersecurity is the protection of cyber-infrastructure from cyber-attacks.

Cyberweapons

In this first section, I discuss the threat to national cybersecurity in terms of the use of 'cyberweapons.' Cyberweapons are software programs designed to attack and damage other software (or data within computer systems) with the intention of doing harm. In this, I follow Neil Rowe's (2010) definition of a cyberweapon in which he argues that cyberweapons are software used to attack other software or data within computer systems.[3] Implicit in Rowe's definition comprises the idea that cyberweapons, by virtue of being an attack on software, are attempting to damage the targeted software in some way.

Cyberweapons might damage software in a variety of ways. A cyberweapon might infiltrate—or inject—unwanted data into an information processing system that alters the database. It might also interfere with intended ways of processing that data, such as is the case with malware, and there are also cases in which the information flow within an information system is blocked, and the degradation or otherwise modification of that flow.[4]

But cyberweapons are designed to do more than simply damage software. Attacks using cyberweapons are 'intentional attacks' that are instigated or controlled by individuals, political organisations—or their military services—with the intention of harming other persons, political organisations or military services.[5] So the purpose of a cyberweapon is to attack an information system in order to perpetrate harm. Stuxnet is frequently cited as a paradigmatic example of a cyberweapon. Discovered in June 2010, Stuxnet is a computer worm specifically designed to attack, and physically damage, Iran's nuclear facilities.

1 ACG. 'Strong and Secure: A Strategy for Australia's National Security.' Canberra: Australian Commonwealth Government, 2013.
2 Joshua, Kopstein, "Cybersecurity': How Do You Protect Something You Can't Define?' The Verge, http://www.theverge.com/policy/2012/8/22/3258061/defining-cybersecurity-fud-cispa-privacy.
3 Neil C Rowe, 'The ethics of cyberweapons in warfare,' *International Journal of Technoethics* 1, no. 1 (2010): 21.
4 Randall R. Dipert, 'Other-Than-Internet (OTI) Cyberwarfare: Challenges for Ethics, Law, and Policy,' *Journal of Military Ethics* 12, no. 1 (2013): 41.
5 Randall R. Dipert, 'The Ethics of Cyberwarfare,' *Journal of Military Ethics* 9, no. 4 (2010): 398.

Cyberweapons pose a number of unique challenges for thinking about the ethics of conflict. First of all, it is difficult to determine the source of an attack using a cyberweapon. The 'attribution' problem, as it is described, is the difficulty of identifying the source of a cyber attack with sufficient certainty to respond. To be morally justified in using a forceful response—especially one that causes significant harm to another party—a necessary condition is that the defender knows the alleged attacker intended to cause harm in some way. Yet the necessary components of cyberweapons—ie, a laptop and an internet connection—are readily available to most people. Expert actors operating from cyberspace do not need significant institutional support potentially to inflict significant amounts of damage on national information networks or infrastructure. So attributing an attack from a cyberweapon to a specific party is notoriously difficult.

A second challenge of cyberweapons is the possibility that they will lower the threshold for conflict between states. The perception that cyberweapons are not seriously harmful could lead to their increased use and potentially instigate more serious forms of conflict. It might prove that many of these threats are not that serious, but the ever-increasing reliance on cyber systems means that cyber-attacks on software can damage critical infrastructure and threaten the lives of people.

Third, cyberweapons increase the likelihood of civilians being targeted and/or becoming victims of disproportionate attacks on joint-use infrastructure. The problem here is that the distinction between joint-use and civilian information systems is much less meaningful when the military use of civilian cyber-infrastructure is ubiquitous.

The war context

Next I demonstrate the way in which the permissibility of using cyberweapons—or responding to an attack from a cyberweapon—is determined by context. My starting point is the presumption that the use of a cyberweapon should be morally justified. In this, I agree with the view that,

> cyber conflict, just as any form of armed conflict or use of force, should only be prosecuted for a compelling and justifiable reason, and only after all reasonable attempts short of these normally-prohibited measures have been attempted without success. We would, moreover, reasonably expect ourselves and others engaging in this form of conflict … to do so only if the ends sought bore some reasonable relationship to the harm and destruction we might otherwise inflict in an effort to resolve the given conflict in our favour.[6]

The basis for this justification, according to Lucas, is meeting the Just War principles of proportionality, discrimination and last resort. In other words, one must prove, first of all, that the use of the cyberweapon is necessary in some way. Second, the use of a cyberweapon should be discriminating in that it is correctly targeted against its intended object. Third, the use of a cyberweapon should be proportionate, in that it does the least amount of harm to achieve its purpose.

6 George R. Lucas Jr, 'Jus in Silico: Moral Restrictions on the Use of Cyberwarfare,' in *Routledge Handbook of Ethics and War: Just War Theory in the 21st Century*, ed. Fritz Allhoff, Nicholas G. Evans and Adam Henschke (Taylor & Francis, 2013), 20.

So what does this mean in practice? Let me attempt to demonstrate using a hypothetical example. Let us imagine that the attacking country launches an unjustified serious cyber-attack on a defending country. This attack attempts to damage the defending country's critical infrastructure (e.g., electricity grid, air traffic control systems) in a way that will seriously harm the inhabitants of the defending country. In this case, a plausible approach to the permissibility of using cyberweapons might run along the following lines:

Necessity: The defending country's use of cyberweapons against the attacker is justified as necessary because it is acting in self-defence, either to halt the attack or to deter the attacker from further hostilities.

Discrimination: The defender might not have conclusive evidence of the attacking country's complicity in the attack, but the seriousness of the threat gives the defender a high-level of leeway in what it targets.

Proportionality: Likewise, the context of the situation allows the defender to inflict a significant amount of harm in response to the attack.

This is what is conventionally described as a 'war' context. The conventional war context presupposes that a damaging act inflicted with the intention of harm is part of a larger struggle between two or more political communities engaged in armed conflict. That is, the incident is classifiable as an armed conflict and part of a war-fighting effort. This means that the decision to use—or refrain from using—force occurs within, and must be judged in terms of, an environment vastly different to what we would expect within a non-war context.

Non-war contexts

Now let us turn to discuss non-war contexts. In most cases, the threats found in cyberspace are more mundane than ruining critical infrastructure or hijacking drones. Most cyber-attacks are best described as cybercrime. These include: spam rings, extortion, money laundering and other organised criminal activity. For these threats, law enforcement is the more appropriate context for conceptualising cybersecurity; and this involves different actors with different reach, jurisdictional boundaries and purposes.

The conventional law enforcement context describes an environment where a sovereign state—or similar political community—is reasonably effective at managing violent conflict within its own jurisdiction using a common body of law. It presupposes at least a basic form of government with a functioning law-making body, criminal justice system and policing institutions. It also requires the absence of serious armed conflict, especially recurring violent incidents between large politically motivated groups. Within the law enforcement context, belligerents who are party to a conflict are treated as suspected criminals and not as combatants.

The conventional understanding of violent conflict within the law enforcement context assumes three basic environmental—or contextual—conditions. First, the conflict is a domestic rather than an international issue. This means that any given state is responsible for resolving a violent conflict that occurs within its own jurisdiction. Second, it is generally assumed that the parties to a violent conflict are non-state actors and the role of the state is to adjudicate fairly between them. Third, the incident is not classifiable as an armed conflict or part of a war-fighting effort.

Having briefly highlighted the war context and the law enforcement context, there is also the sometimes discussed murky world of cyber espionage. According to Dipert,[7] attacks in this realm include, "traditional counterespionage and disinformation campaigns, old-fashioned destruction of telephone lines, jamming of radio signals, killing of carrier pigeons, and so on." He goes on to suggest that espionage is not usually an activity that has been considered part of the moral considerations in regard to conventional conceptions of Just War Theory, and that the ethical considerations in espionage and other intelligence-gathering operations are but one of the several traditionally neglected aspects within the morality of conflict.[8]

Let us consider a second example to illustrate the point that our interpretation of the basic moral principles for using cyberweapons should look considerably different in non-war contexts. Imagine a second example in which a group working from the attacking country steals sensitive information from the defending country, but with little or no damage to the defender's cyber infrastructure and no threat to the inhabitants of the defending country. In contrast to the first example,

Necessity: Perhaps it is possible that the defender is justified in using a cyberweapon in this case, but it would require some other key factor. For example, the attacker might be stealing sensitive information as part of its preparation for a military attack on the defender.

Discrimination: Even if the use of a cyberweapon is somehow justified, we would require more stringent proof as to the identity of the perpetrators.

Proportionality: We would also want the harm to be strictly localised to the target in question.

Conclusion: the war-fighting distinction

In conclusion, the point of this exercise is to demonstrate the importance of what I refer to as the 'war-fighting' distinction for determining the application of moral principles in conflict. The war-fighting distinction states that designating a context as 'war' alters the way in which we should interpret the basic moral principles for justifying the use of cyberweapons, or responding to being attacked by a cyberweapon. In this case, there is an important moral distinction to be made between attacks using a cyberweapon and one that is designed for the purposes of cyber exploitation. And the reason for the importance in accurately describing cyber-attacks is because "there is always a risk of escalating a case of espionage or crime to international armed conflict."[9]

In other words, we do not want states overreacting to cyber-attacks. The key mistake here is to conflate the threat from a cyber-weapon with one that involves 'cyber exploitation.' There are non-damaging cyber-attacks that aim to exploit an information system without causing harm. Examples include: 1) theft of information, both state-sponsored and criminal; 2) creating unauthorised access to a system; or 3) attempts to take control of an information system. The important point here, so the reasoning goes, is that we should acknowledge an important distinction between attacks using cyber-weapons, which, as I have argued, aim to harm infrastructure and persons, and cyber-exploitation, which involves a non-damaging attack on cyber-infrastructure, and then respond accordingly. Consequently, the permissibility of using cyberweapons in response to a cyber-attack is contingent upon the context of the threat.

7 Randall R. Dipert, 'The Ethics of Cyberwarfare,' *Journal of Military Ethics* 9, no. 4 (2010): 386.

8 Randall R. Dipert, 'The Ethics of Cyberwarfare,' *Journal of Military Ethics* 9, no. 4 (2010): 389.

9 Panayotis A Yannakogeorgos. 'Keep Cyberwar Narrow.' *The National Interest*, http://nationalinterest.org/commentary/keep-cyberwar-narrow-8459.

Australian National University

National Security College

Policing cyber-threats:
Regulating exceptional police actions[1]

Adam C Gastineau

National Security College

The National Security College is a joint initiative of the Commonwealth Government and The Australian National University

Introduction

As with any type of surveillance, the challenge for security services is to balance the need to detect and interdict threats to the community against the rights of the community that they are meant to protect. Cyber-surveillance grants security services great power in both collecting and collating information, allowing state agents to form highly detailed profiles of individuals or groups by using a wide range of sources of digital information. However, as the recent controversy with the US National Security Agency has revealed, states cannot expect to have *carte blanche* in the use of such technology. The central claim of this section is that policing activities in the cyber sphere can prove to be as great an issue of moral concern to a population, particularly the populations of liberal democracies, as the activities of those seeking to undermine the state or actively attempting to harm the populace. As technology increases our ability to access each other's lives, we become more capable of affecting, directly or indirectly, the actions of others. Insofar as we hold certain political goods (e.g., freedom) and personal goods (e.g., autonomy or individual liberty) to be valuable, we have reason to ensure that this increased power granted to the state to conduct general surveillance of its populace is carefully regulated. Failing to do so would allow for large-scale privacy violations, and with these violations large-scale ethical violations against those living within such societies.

This paper will proceed as follows: First I provide a brief overview of what exactly I mean when discussing 'Cyber' (or 'Cyberspace') and Cyber-surveillance. Second, I outline the ostensibly neutral definition of privacy given by Ruth Gavison. This definition defines privacy as being an issue of accessibility rather than one of control, and I offer a brief summary of the reasons behind this. Next I briefly examine why we might think that restrictions of privacy are ethically problematic. Finally, I apply this analysis to the issue of cyber-surveillance to argue that societies that claim to value freedom and individual rights should place strong restrictions on the use of such technology by the state. I then briefly outline what these restrictions might look like, and explain when the state might be ethically justified in using such technology.

Cyber-surveillance and privacy

Before discussing privacy, some account of 'cyber-surveillance' is necessary. Some current cases include: surveillance of populations via network-enabled devices, such as travel information gleaned from 'smart cards' by Victorian Police[2] and the NSA, using large amounts of data from major internet providers to identify and track particular targets; and the possible use of drones by law enforcement agencies to collect evidence for use in later prosecutions. The term 'cyber' or 'cyberspace' has not yet been formally defined, though there is some general agreement in the literature. One might traditionally define 'cyberspace' as the existing set of interdependent, networked communications and information technology systems. Such systems include the internet and all that is associated with it, incorporating online social networking sites, e-mail, phones, SMS/text, and GPS. Also included are systems that provide services facilitated by the internet and other similar networks. These public cyber systems include transport key cards or 'e-tags' that track a user's activity on various public transit systems or roadways, and charge the user's account accordingly. Also included in this set would be commonly used security tools such as CCTV cameras and license plate/traffic cameras. Such systems collect a very narrow set of data, which is then indexed and stored.

1 References to 'just' or 'unjust' refer to ethical, not necessarily legal justification. Such claims may or may not also apply to legal justifications. As such something maybe permitted by law but not ethically 'just' by this analysis.

2 Thomas Hunter, 'Myki is Watching You: Smartcard Operator Gives Police Access to Customer Info', *The Sydney Morning Herald*, (2010)., Neil Rees, et al., 'Surveillance in Public Places', (Victorian Law Reform Commission, 2010), 180.

When these narrow data sets are combined and used in conjunction with other cyber systems, however, they can be used effectively to monitor individuals. By collating these various narrow data streams one can determine movement patterns, identify vehicles or other forms of transport commonly used, and other habits. Cyber technology allows one to create a comprehensive picture of an individual and their habits in a relatively short time.

It is not my intention here to go into any great detail on the various debates that have sprung up in the privacy literature. Nonetheless, a concept of privacy in some form is necessary for the discussion. Certain assumptions will be made, but these should not have a great effect on the claims I wish to make regarding the limits to be placed on police powers in liberal democracies. Though the divergent views inherent in the varying conceptions of privacy may be at odds with one another, given a neutral approach to privacy, the conclusions drawn should remain the same.

Ruth Gavison has offered what she terms a 'neutral' definition of privacy.[3] This definition seeks to outline the characteristics of the term without exploring why privacy neutrality of terminology might be valuable. As such, it is primarily a functional description of what we are talking about when we consider privacy, and in particular violations of privacy. Gavison points out that when we are discussing issues of privacy we are referring to our 'accessibility to others' and she breaks this accessibility into three main categories: information/secrecy, attention/anonymity, and access/physical access.

First, 'information' is precisely that: data about ourselves. The greater access one has to data about an individual, the greater the reduction in privacy. If I have access to information about an individual I may use that data to forecast behaviour, track the individual, or gain access to additional data, such as accessing bank records or e-mail accounts. In gaining information about an individual, I gain access to them as an individual even if I never actually interfere with them at all.

Second, Gavison splits 'attention' into two sub-categories. One may think about an aspect of a particular individual. For example, I might think about what Tony Abbott is likely to do on his days off; what kind of beer he most likely drinks; where he goes; who he may see, and so on. Gavison argues that my paying this kind of attention to Tony Abbott does not violate his privacy, since this sort of speculation, on its own, gives me no real access to him. But there is another type of attention that one might pay to an individual, which would constitute an invasion of their privacy. This is what I will call 'actualised' attention. This kind of attention is not merely focusing one's thoughts on an individual and speculating about them, but actually watching, tracking, or otherwise monitoring an individual as they go about their daily lives.

Finally, Gavison points out that one considers one's privacy to be violated when an agent is able to gain 'physical access' to us without our consent. By physical access Gavison means that one is able to place themselves in close enough physical proximity to an individual that they are able to observe that individual by means of their regular senses. For example, a 'peeping tom' who stations themselves outside an individual's windows to watch them undress violates the individual's privacy in this way.

These three characteristics are interrelated, but conceptually independent of one another. I might gather information on an individual without ever focusing my attention on the individual themselves or being in close physical proximity to them. Likewise, I might observe an individual closely, staring at someone at the next table in a café, without acquiring any further information about them. Finally, peeping toms may restrict another's privacy by positioning themselves outside the window, as in doing so they give themselves physical access to that individual without the individual's permission even if the individual is not yet in the room. In many cases, however, these three characteristics of accessibility are interrelated and feed one another.

3 Ruth Gavison, 'Privacy and the Limits of Law,' *The Yale Law Journal* 89, no. 3 (1980).

Privacy as Accessibility

For example, take a standard case of a stalker. The stalker notices the individual in a café, and watches the individual closely, following them as they leave and walk to a particular address. Using this information the stalker obtains information about the person who lives or works at this address, accessing their Facebook account or tracking them through social networks and monitoring their movements online. Finally the stalker adopts a position from which to observe their subject without their knowledge, placing themselves outside their target's window when they know the target to be elsewhere in order to watch them when they return. Here one can see how actualised attention garners information, which allows for further actualised attention—more information—and finally physical access to the individual targeted.

The value of privacy[4]

Privacy is valuable for at least three reasons. First, privacy acts as a restraint against the state dominating its citizens, thus protecting citizens' freedom from state power. Second, having a sphere of privacy, wherein no one can gain access to me without some justification, reinforces my status as an autonomous individual. Third, insofar as this sphere of privacy is important to me as an autonomous individual, one has a strong claim that it not be violated without sufficient justification. All three of these claims about privacy are extensively discussed in the ethical literature on the subject. In the interests of space I will only address the first of these reasons here.

Philip Pettit formulates a concept of freedom[5] on the difference in power between agents. Pettit suggests that freedom is a sort of 'anti-power.' In order for an individual to be free, others must not have the power to dominate that individual. One is dominant over another if, and only if, one has an actual capacity to interfere with the dominated individual, can do so without penalty, loss, or chance of the subjugated individual asserting themselves in response, and can do so within a certain sphere of choice.[6]

Pettit's account maintains that provided these three conditions are met, it is irrelevant if the dominating party chooses to interfere with the subject or not. The mere fact that the dominator could do so is sufficient to support the claim that the subjugated agent is not free. Pettit has also pointed out that this anti-power, or lack of dominance, must be robust if it is to constitute freedom. If one might be dominated at one point in time, but not another, based on the whim of the potential dominator, then one is not actually free. In short, if there is a 'door-keeper' on which one's 'freedom' is contingent, then one is not in fact free. Liberal democracies that stress the importance of freedom must therefore ensure that the policies and legislation they pursue preserve this freedom by preventing the state dominating the individual in this way.[7]

4 For accounts discussing the importance of privacy to the autonomous individual, see Jeffrey H. Reiman, 'Privacy, Intimacy, and Personhood,' *Philosophy & Public Affairs* 6, no. 1 (1976); Joseph Kupfer, 'Privacy, Autonomy, and Self-Concept,' *American Philosophical Quarterly* 24, no. 1 (1987). For accounts discussing privacy as a right, see the following: Judith Jarvis Thomson, 'The Right to Privacy,' *Philosophy & Public Affairs* 4, no. 4 (1975); Thomas Scanlon, 'Thomson on Privacy,' ibid; Thomas Nagel, 'Personal Rights and Public Space,' ibid.24, no. 2 (1995).

5 There are many accounts in ethical literature and political theory of what exactly constitutes 'freedom'. This is only one of these accounts. For other accounts of freedom as non-interference see Thomas Hobbes, *Leviathan* (1651); J.S. Mill, On Liberty (Oxford: Oxford University Press, 1991); and, more recently, Robert E. Goodin and Frank Jackson, 'Freedom from Fear,' *Philosophy & Public Affairs* 35, no. 3 (2007).

6 '…(1) has the capacity to interfere (2) with impunity and at will (3) in certain choices that the other is in a position to make.' Pettit includes manipulation as a form of interference. Philip Pettit, 'Freedom as Antipower,' *Ethics* 106, no. 3 (1996).

7 Phillip Pettit, 'The Instability of Freedom as Noninterference: The Case of Isaiah Berlin,' *Ethics* 121, no. 4 (2011).

Implications for police surveillance

Cyber-systems increase the capability for an agent or agency to gain access to individuals. In some cases, as with drones or security cameras, such technologies may make it easier to focus our attention on an individual or group we wish to monitor. However, these technologies help us in other ways as well. Nissenbaum[8] has pointed out that data gleaned from focusing our attention is sporadic and disjointed, and therefore difficult to analyse in many ways. This is no longer the case when drones and other cyber technologies are used, particularly when used in tandem with information obtained from monitoring other cyber systems such as meta-data, smart cards, and e-tags. These technologies allow us to connect small pieces of information to one another and collate them into a comprehensive picture of an individual, allowing us greater ability to interfere with that individual as they go about their daily lives, and thereby reduce their freedom.

Think back to our stalker case and substitute a police officer, or other state agent, for the stalker. You are sitting peaceably in a café when you notice a uniformed police officer watching you, staring at you. This might be mildly disturbing, but not catastrophic. Now imagine that as you leave you notice the officer following you to your car. As you drive off you notice a police car behind you in traffic, which stays there until you arrive at your destination. At various times during the next week you notice police driving by, or officers watching and perhaps following you when in public. So far we have only addressed one aspect in which privacy might be violated: attention. Now imagine you discover that the government has gained access to various pieces of data such as those mentioned above, and is using that data to further focus its attention on and gain physical access to you. This data might be meta-data logging the location and time of phone calls you have made or e-mails that you have sent, who received them and when. Such data might also include your browsing history on the internet or membership of certain online forums. Perhaps, you discover that the police have gained access to smart-card records kept by the public transport systems that record the stops at which cards are used on public transport, or have tracked the times and dates you have passed certain toll stations. All of these fall into the second aspect of privacy above: access to information. Finally, let us incorporate the third aspect of privacy: physical access. One day, after several weeks of being watched you arrive home. You've not been followed, but sitting across the street from your house is an official-looking car with a suited individual in the front seat. Later that evening you notice the same individual standing outside your house watching you as you move around inside your home. Such a situation would likely make one particularly uncomfortable and would certainly affect the decisions one might make. One might avoid certain neighbourhoods or groups that one believes to be considered dangerous by the state whether you believed them to be dangerous or not. One might not engage in certain activities that are legally or socially unacceptable, even if only trivially so. For example, one might pay much more attention to one's speedometer to observe the speed limit, and might not visit bars in a red-light district or in gathering places for those with ideas that ran against the social norm.

This scenario demonstrates how state surveillance, without the restrictions suggested here, could reasonably result in changes to an individual's behaviour due to state surveillance that amount to domination by the state and so a violation of their liberty. This is not to say that surveillance is never permissible. Such restrictions seem perfectly reasonable if one has chosen to act in a way that designates them as a threat to others, by choosing to speed while driving for example, or choosing to behave recklessly in public. However, insofar as such surveillance targets individuals who have not chosen to engage in such behaviour, it violates their privacy, and insofar as such violations affects the choices they might permissibly make, it restricts their freedom without justification.

8 Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life,* (Stanford University Press, 2009).

To highlight a case of particular concern, members of ethnic or religious groups that are considered to be risky in some sense by the state may be less likely to engage in activities considered permissible for other groups: choosing not to attend political, religious, or social events they would otherwise wish to attend because they fear that doing so will expose them to greater invasions of privacy or open them to other forms of state interference. Presuming that one has no choice in membership in such groups, these individuals are not liable to state surveillance, or accompanying restrictions in freedom, because they themselves have yet to demonstrate that they are a threat.

In cases where there is some choice, as in association with specific religious institutions or social organisations or clubs, some surveillance may be permitted of these institutions, organisations or clubs. However, further surveillance of individual members may or may not be permissible. Those who have chosen to behave as a threat as defined above are liable and therefore targetable because of this choice, but according to the analysis presented here, those who cannot be shown to have made such a choice are not subject to such surveillance as it violates their privacy and thereby unjustly restricts their freedom. Police surveillance is greatly enhanced by advances in technology. However such advances are only as valuable as long as they are used to preserve those values, like liberty, that are held to be most important in society. When they are used in a way that damage such values, regulation is necessary to maximise the benefit of these advances for all.

Insofar as one gains access to another, one restricts their privacy. Insofar as we restrict their privacy, we restrict their freedom. But surely this is not always a bad thing. There are plenty of cases in which such reductions of freedom might be permissible. How then do we determine which privacy restrictions are permissible and which are not? In cases where the target being monitored is acting, or perhaps has recently acted, in a way that makes them liable to be so monitored, then the individual loses their claim, to some extent, to privacy and must bear the requisite loss of freedom that results.

How then do we determine who is liable and who is not? Here I turn to a recent RAND Europe report on cybersecurity, which seems to offer a solution.[9] In this report RAND analysts offer a distinction between Risks and Threats. Risks are a function of possible threats multiplied by vulnerability to such threats, multiplied by the severity of the possible outcome should the threats eventuate. Threats, on the other hand, consist in a 'motivated adversary who exercises choice.' Risks then are general in scope, whereas threats, in contrast, require a specific 'adversary' that behaves in a certain way. Because threats constitute wilfully acting in an 'adversarial' manner, they pose a greater risk of harm, and so are liable to have their privacy violated, and freedom restricted, by security surveillance in proportion to the threat they pose. To clarify this last point somewhat consider the following example: All else being equal, a person carrying a firearm constitutes some risk to others. However, when the individual wilfully acts in an 'adversarial' manner, by drawing the weapon and pointing it at some other agent, or indicates some motivation to harm by leaving the weapon holstered while verbally threatening others with harm, or perhaps even just shouting aggressively at others while gripping the weapon or displaying the weapon in its holster, it seems reasonable to say that the individual poses a greater risk of harm: a threat.[10] The individual becomes liable to have greater restrictions placed on their freedom, such as being subject to surveillance by the state, for at least as long as such behaviour is manifest, because they choose to behave in this fashion. Risks on the other hand, are not liable to be so restricted, precisely because they lack the active motivation and choice necessary to become liable. In short, while they might become a threat sometime in the future, they are not yet a threat and so are not permissible targets for state surveillance. This then makes any such surveillance a violation of their privacy, thereby unjustly restricting their freedom.

9 Neil Robinson et al., 'Cyber-Security Threat Characterisation: A Rapid Comparative Analysis,' ed. RAND Europe, Cambridge, UK, 2013.

10 Of course there may be some disagreement about when the risk posed by an individual agent is sufficiently elevated for that individual to be considered a threat. However, it is sufficient for the discussion here to give some idea about how one should go about drawing the line, even if space requirements do not allow for argument about precisely where that line should be drawn.

Conclusion: restraining police surveillance

This analysis rules out giving police and other state security agencies broad access to data pertaining to those living within the state. It also requires that some sort of third-party evaluation is necessary in cases where the police believe a threat to exist, to ensure that the target of that surveillance is not merely an individual or group posing a risk, but rather one that constitutes a threat to the community. This evaluation currently takes the form of judicial review of such cases, with a warrant, or similar legal mandate required before surveillance is undertaken. It seems to me that these precedents should be applied to police use of 'cyber-surveillance' as well. As cyber technologies advance, however, such restrictions and oversight must take into account the increased capability these technologies offer to invade the privacy of individuals, as states that claim to value freedom cannot morally restrict the freedom of their citizens without good cause.

Australian National University

National Security College

Virtual terrorism:

Data as a target

Levi J West

National Security College

The National Security College is a joint initiative of the Commonwealth Government and The Australian National University

Introduction

The conceptualisation of cyberterrorism is by its inherent nature contested, opaque and, at times, wilfully inaccurate. Engaging in a structured analytical process that seeks to establish some degree of conceptual clarity in regards to this concept is essential so as to ensure that public policy responses and broader security discourse in relation to cyberterrorism remain proportionate and necessary and, crucially, effective. This paper identifies the dominant approaches to the concept of cyberterrorism and highlights some of their key shortcomings. Further to this, the paper hypothesises actions and behaviours that could accurately be described as cyberterrorism, and through use of alternatively proposed language suitably depict malicious behaviour occurring in or through cyberspace. By drawing on central works in relation to the definition of both 'cyber' and 'terrorism', this paper seeks to identify potential new sites for ideologically motivated activity that targets and/or leverages cyberspace. In doing so, it is hoped that emergent activities and possible future incidents may be conceptualised in a more accurate, moderate and informed manner, ensuring appropriate responses.

First of all, it is necessary to address the definitional problems in the term 'cyberterrorism'. As many scholars of terrorism and political violence readily acknowledge,[1] there is no universally accepted definition of terrorism, either in legal, policy or conceptual terms. Schmid states in the introduction to his chapter on defining terrorism that:

> There are hundreds of definitions of terrorism in use …. They emphasize a variety of attributes of terrorism …. Yet such a listing of frequent and similar elements of terrorism is in itself not a definition.[2]

The challenge that this presents for analysing cyberterrorism is substantial in that it presents a contested concept—'terrorism'—and merges it with the emergent, contested, and ill-defined term 'cyber'. This permits the term to be used to refer to incidents that have little or no correlation to terrorism in either the strict or broad sense, and no necessary or specific relationship to the security risk dynamics of 'cyber.' As Brookings Institution Senior Fellow Peter W. Singer stated in 2012:

> About 31,300. That is roughly the number of magazine and journal articles written so far that discuss the phenomenon of cyber terrorism. Zero. That is the number of people that who (sic) been hurt or killed by cyber terrorism at the time this went to press. In many ways, cyber terrorism is like the Discovery Channel's 'Shark Week,' when we obsess about shark attacks despite the fact that you are roughly 15,000 times more likely to be hurt or killed in an accident involving a toilet.[3]

The ambiguity that cyberterrorism embodies provides a powerful rhetorical device that enables politicians and senior policy makers to engage in securitisation acts that potentially creates unwarranted—or misconstrued—responses to securing cyberspace, potentially resulting in the misdirection of national security and law enforcement resources. In consideration of this risk, cyberterrorism warrants appropriately structured and focussed analysis.

1 See Schmid, A.P. (2012). 'The revised academic consensus definition of terrorism'. *Perspectives on Terrorism*, 6(2), 158-159. Available: http://terrorismanalysts.com/pt/index.php/pot/article/view/schmid-terrorism-definition; Weinberg, L., Pedahzur, A. & Hirsch-Hoefler, S. (2004). 'The Challenge of Conceptualizing Terrorism', *Terrorism and Political Violence*, 16(4), 777-794'. Available at: http://dx.doi.org/10.1080/095465590899768; Ganor, B. (2002). Defining terrorism: Is one man's terrorist another man's freedom fighter? *Police Practice & Research: An International Journal*, 3(4), 287-304. http://dx.doi.org/10.1080/1561426022000032060

2 Schmid, A.P. (2011). *The Routledge Handbook of Terrorism Research*, London, UK: Routledge, p. 39.

3 Singer, P.W. (2012). 'The Cyber Terror Bogeyman'. *Armed Services Journal*, 12. Available here: http://www.brookings.edu/research/articles/2012/11/cyber-terror-singer

The conceptual and definitional problem

At the core of the ambiguity regarding 'cyberterrorism' are the misconceptions relating to its component terms: 'terrorism' and 'cyber.' First, terrorism is an ideologically and politically contested term. For every instance in which an act is appropriately described as terrorism, there are instances in which the term is deployed for political or ideological advantage. As Young states, "Generally speaking, for hundreds of years 'terrorism' has been used as a pejorative term, usually applied to 'the other side.'"[4] As such, terrorism remains contested, ill-defined and difficult to objectively verify, a problem that has been exacerbated by the heightened sensitivities of the post-9/11 era. This absence of conceptual clarity makes effective analytical approaches to terrorism complex, as it does the development or refinement of related concepts.

Second, the 'cyber' prefix is also problematic. It has come to be applied to a broad, emergent subset of security discourse; it lacks conceptual clarity and in many cases is simply inaccurate. The etymology of the word comprises distinct disparities across its current forms of usage, with reference to a number of security related issues tending to confound rather than clarify. As Ottis identifies:

> In recent years the term 'cyber' has been used to describe almost anything that has to do with networks and computers, especially in the security field … including state-on-state cyber warfare, cyber terrorism, cyber militias etc. Unfortunately, however, there is no consensus on what 'cyberspace' is, let alone what are the implications of conflicts in cyberspace.[5]

One of the earliest efforts to establish something akin to a definition of cyberterrorism can be seen in the work of Denning,[6] who initially refers to the 'convergence of cyberspace and terrorism.'[7] The simplicity of this approach is appealing, but it depends on what have just been demonstrated as contested and unclear terms.

Predominant approaches to cyberterrorism

The increased focus of both government and of academia on matters pertaining to cyberspace and cybersecurity has led to an expanded body of literature that seeks to provide some degree of clarity on cyberterrorism. With this have come distinctions between different manifestations of a definitional convergence. This emerges, in part, from critical approaches by scholars specialising in terrorism research, and also from those researchers who have the technical capability to assess the plausibility of the scenarios that are often articulated as manifestations of cyberterrorism. The following identifies both the primary articulations of cyberterrorism and some of the shortcomings of these conceptualisations.

4 Young, R. (2006). 'Defining Terrorism: The Evolution of Terrorism as a Legal Concept in International Law and Its Influence on Definitions in Domestic Legislation'. *Boston College International and Comparative Law Review*, 29((1), 23-105.

5 Ottis, R. and Lorents, P. (2010). Cyberspace: Definition and Implications'. In Proceedings of the 5th International Conference on Information Warfare and Security. Dayton, OH, US: Academic Publishing Limited, p 267-270. Available here: https://docs.google.com/file/d/0B7yq33Gize8yOGY0MGYwODEtODViZi00YTliLTg5ZjYtNTc3NDZmOGFjNDVi/edit?usp=drive_web&urp=http://conflictsincyberspace.blogspot.com.au/p/pub&pli=1&hl=en#

6 Denning, D.E. (2001). 'Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for influencing Foreign Policy. In Arquilla, J. & Ronfeldt, D. (eds.) *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, USA: RAND Corporation, p. 239-288.

7 *Ibid*, 241.

Some of the earliest and most enduring articulations of cyberterrorist acts centre upon attacks on critical infrastructure.[8] This particular variant of thinking in regards to cyberterrorism can be seen as a logical reflection of the ongoing convergence of the physical and virtual worlds, and the increased role that computer systems and computer networks play in managing, regulating and controlling systems that provide critical utilities and resources to citizens of advanced economies. In conjunction with a number of other drivers—such as the economically motivated advent of just-in-time inventory and the globalisation of production processes—social and economic infrastructure is portrayed as part of a fragile and vulnerable system. Social survival is seen as increasingly reliant on this system, thus presenting an attractive target for a cyberterrorist.

But there exists some key flaws in these apocalyptic scenarios, which envisage the total collapse or impairment of a society's critical infrastructure. They are as much manifestations of the securitisation of cyberspace generally as they are a consequence of the failure to understand the potential reality of cyberterrorism. Partly as a function of the types of scenario planning and horizon scanning exercises of the likes of Collin and Denning, and especially in the counterterrorism environment of post-9/11, much of the vulnerable critical infrastructure has been appropriately hardened for defensive purposes. By 2004, a range of government departments—in the United States, generally conceived of as both the most vulnerable and the most likely target—had taken defensive countermeasures in seeking to address vulnerabilities in their systems. Additionally, a range of industry participants had also sought to minimise the likelihood of cyber-attacks on their assets.[9] While recent cyber-attacks—such as Stuxnet and its variants—suggest that it remains plausible to launch code-based attacks on infrastructure, the scale, cost, specificity and complexity of this incident[10] makes it unlikely that a similar incident will be undertaken by a terrorist actor. Furthermore, it seems unlikely that even a successful cyberterrorist penetration of a critical infrastructure control system would achieve the types of objectives sought by terrorists. After applying a cost-benefit analysis approach to cyberterrorism, Giacomello determined that "even for a well-funded terrorist organization cyberterrorism would not be a cost effective operation."[11]

The second approach to cyberterrorism focuses on terrorist *use* of cyberspace, primarily the Internet. This approach considers the terrorist use of cyberspace as a safe haven and as a distributed command and control network. The proliferation and accessibility of terrorist literature presents a much higher return on investment than the highly specific and technical requirements required for critical infrastructure attack. Additionally, use of cyberspace to distribute extremist literature and propaganda, and as a recruitment tool,[12] provides longevity and sustainability to a terrorist movement while also enhancing the network's resilience. If a comparison is undertaken of the costs and risks of operating physical training camps with the costs and risks of publishing al Qaeda in the Arabian Peninsula's global jihadist magazine *Inspire* online, the use of cyberspace for propaganda and recruitment purposes clearly offers a more effective strategy. In some senses, this approach is linked to counterterrorism efforts. The destruction of physical training camps has forced terrorist actors—especially al-Qaeda—to move much of their operational efforts into cyberspace. It is important, however, to recognise that there is also a body of doctrinal work that underpins and supports these efforts, and al Qaeda in particular have sought to leverage the operational security benefits of networked structures and distributed command and control.[13]

8 Collin, B. (1997). 'The Future of Cyberterrorism. Crime and Justice International', 13(2), 15–18. Available: http://www.cjimagazine.com/archives/cji4c18.html?id=415

9 Shea, D.A. (2004). *Critical Infrastructure: Control Systems and the Terrorist Threat*. (CRS Report RL31354).

10 Sanger, D.E. (2012). 'Olympic Games'. In *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York, USA: Crown Publishers, 188–225.

11 Giacomello, G. (2004). 'Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism'. *Studies in Conflict and Terrorism*, 27(5), 387-408. Available here: http://dx.doi.org/10.1080/10576100490483660

12 Seib, P. and Janbek, D.M. (2011). *Global Terrorism and the New Media: The Post-Al Qaeda Generation*. London, GBR: Routledge.

13 Sageman, M. (2008). 'Terrorism in the Age of the Internet'. *In Leaderless Jihad: Terror Networks in the Twenty-First Century*. Philadelphia, PA, USA: University of Pennsylvania Press, p. 109-124.

Why are these not cyberterrorism?

Both of these approaches to cyberterrorism suffer from problems, however. Although cyber-attacks on critical infrastructure appear to be a reasonable description of something akin to cyberterrorism, there are a number of complicating factors. First, most critical infrastructure, and especially that which has been deemed to be crucial to the ongoing viability of the state, has been hardened and has protocols that seek to ensure any type of cyber-attack is unlikely to be successful or cannot cause serious harm. Further to this, there is the reality that many attacks on these types of assets may be undertaken for other than political or ideological motivations, which are conditions necessary to qualify them as cyberterrorism attacks. The more serious threat is from well-resourced state actors rather than terrorists. The technical challenges required for a serious cyber-attack on critical infrastructure means that this form of cyberterrorism becomes an unlikely, if partly plausible, manifestation of the overall threat in cyberspace.

The second approach to conceptualising cyberterrorism—that of terrorist use of cyberspace for propaganda, recruitment, financing and other administrative-type objectives—struggles to be conceived of in any way as an act of cyberterrorism in and of itself. *Inspire* magazine in and of itself is not a terrorist incident. Its title provides much of the requisite understanding for what its role is in the terrorist attack cycle. The attack inspired by the magazine's content, or the attack sanctioned by email correspondence between terrorist group members and aspiring operatives are not terrorist attacks. The attacks themselves carry this title. The mere involvement or use of cyberspace or computer networks at some point in the attack cycle does not warrant use of the terminology of cyberterrorism, and if deployed to discuss these types of incidents, warrants scepticism as to the purpose of the use of the term.

Conclusion: imagining cyberterrorism

In conclusion, much of the existing conceptualisation of cyberterrorism lacks adequate specificity or refers to tactics that lack adequate return on investment to be likely. So it is worthwhile, in much the same way that scholars and policy makers did in the early 1990s, to envisage an act that might warrant labelling as cyberterrorism. It is here that we can engage in a very brief horizon scanning exercise so as to provide guidance as to what potential manifestations of cyberterrorism may entail.

By recalling some of the key characteristics of terrorism that were discussed at the outset, we can provide a useful and interesting framework through which to conceive future cyberterrorism. Terrorism is, above all else, a communicative act. Violence used by terrorists is a means rather than an end. Understanding that the violence traditionally considered as central to terrorism is instrumental allows us to focus instead on the objectives of terrorism: political or ideological outcomes. It is also useful to identify that Schmid's seminal chapter on defining terrorism identified a number of 'contested elements,' in which some respondents of the survey that informed the work were prepared to 'label certain harmful acts (such as computer hacking) terrorism even when no direct violence is involved or no terror results'.[14]

14 Schmid, *The Routledge Handbook...Ibid*, pg.84

It is worthwhile citing an analogy from current events. Edward Snowden has successfully altered the dynamics of much of the intelligence-gathering practices of the United States intelligence community. He has also impacted the relationship between national governments and, consequently, initiated broad public debate about intelligence practices, intelligence collection and general oversight and accountability. He has achieved this political or ideological objective without detonating an explosive device, without firing a weapon, and without engaging in anything that could be generally constituted as violence. It could plausibly be argued that had he used the types of tactics that a conventional terrorist organisation would have used—such as a car bomb—any form of political discourse regarding the NSA's intelligence collection programs would have failed. It is likely that such an attack would have provided sufficient political basis for an expansion of the programs in place. By not engaging in conventional violence, but by using cyber capabilities and targeting cyber assets—data—Edward Snowden was able to achieve something in regards to what we can deduce to be his political or ideological objectives. This is perhaps the prototypical example of future 'cyberterrorism.' Stealing, corruption, or destruction of data may prove to be a much more effective, low-cost mechanism of coercion that in a further converged world is able to instil 'fear, dread, panic or mere anxiety.'[15] The implications of this kind of attack would be multifaceted and far-reaching, with significant ramifications for numerous aspects of modern life. The capacity to alter significantly individuals' capacities to go about daily life, or to undertake rudimentary essential tasks, or to erase or corrupt their digital existence can only become more terrifying as modern society continues to integrate the virtual world into the physical. Perhaps a future that contains cyberterrorism, with data as a target, is more plausible than initially conceived.

15 Schmid, *Ibid*, p. 86

CONTACT US

National Security College
GJ Yeend Wing (Crawford Bldg #132a)
1 Lennox Crossing
The Australian National University
Canberra ACT 0200
Australia

T +61 2 6125 1544
E national.security.college@anu.edu.au
W nsc.anu.edu.au

CRICOS #00120C